

On the strong converses for the quantum channel capacity theorems

Naresh Sharma^{1,*} and Naqeeb Ahmad Warsi^{1,†}

¹*School of Technology and Computer Science,
Tata Institute of Fundamental Research (TIFR),
Mumbai 400 005, India*

(Dated: March 3, 2013)

A unified approach to prove the converses for the quantum channel capacity theorems is presented. These converses include the strong converse theorems for classical or quantum information transfer with error exponents and novel explicit upper bounds on the fidelity measures reminiscent of the Wolfowitz strong converse for the classical channel capacity theorems. We provide a new proof for the error exponents for the classical information transfer. A long standing problem in quantum information theory has been to find out the strong converse for the channel capacity theorem when quantum information is sent across the channel. We give the quantum error exponent thereby giving a one-shot exponential upper bound on the fidelity. We then apply our results to show that the strong converse holds for the quantum information transfer across an erasure channel for maximally entangled channel inputs.

I. INTRODUCTION

One of the holy grails of information theory has been to prove the information-carrying capacities of various channels [1]. The capacity identifies the maximum rate (measured as number of bits/qubits per channel use) with which one could transfer information reliably across the channel in the limit of sufficiently large number of channel uses [2–7].

The capacity, for certain channels, also told us an interesting property about the fidelity between the message at the source and the replicated message at the receiver and this interesting property is that the fidelity could be made (with appropriate inputs) to go to 1 (i.e., a completely reliable transfer) for rates below capacity and goes to 0 (i.e., a completely unreliable transfer) for rates above capacity for any input for sufficiently large number of channel uses.

Such converse theorems where the fidelity goes to 0 for sufficiently large number of channel uses for rates above capacity are referred to as the strong converses. For certain channels, one could show that the fidelity would decay exponentially to zero as the number of channel uses increases for rates above capacity. An example of a channel with no strong converse is given in Ref. [8].

A strong converse for the classical discrete memoryless channel (DMC) was given by Wolfowitz [9]. In a simpler form, it showed that for rates above capacity, $1 - P_e$ (P_e denotes the probability of decoding error) can be bounded from above by two terms: one that decays as $1/n$ and the other that decays exponentially with n , where n is the number of channel uses.

Arimoto provided a different strong converse with $P_e \rightarrow 1$ exponentially with n using the error exponents [10]. These error exponents were known from the work of Gallager who used them to give an upper bound to show $P_e \rightarrow 0$ exponentially for rates below capacity [11].

*Electronic address: nsharma@tifr.res.in

†Electronic address: naqeeb@tifr.res.in

An important problem in quantum information theory has been to find the capacity of a quantum channel for classical information transfer [12–14]. Winter provided a strong converse which guarantees that for rates above capacity $P_e \rightarrow 1$ as $n \rightarrow \infty$ [15]. Ogawa and Nagaoka gave an Arimoto-like strong converse where they showed that $P_e \rightarrow 1$ exponentially with n [16].

The channel inputs used in the strong converse theorems mentioned above were unentangled across channel uses. In a fully general channel converse, such a restriction would not be made. König and Wehner provide a strong converse for entangled inputs for a subclass of channels for which a single-letter formula for capacity is available [17]. More strong converse theorems not necessarily in the context of channel capacity could be found in Refs. [18–22].

Polyanskiy, Poor & Verdú and Polyanskiy & Verdú (see Refs. [23, 24]) provided a unified converse for the classical channel capacity theorem and such a converse yields among others the Arimoto converse (Ref. [10]), Wolfowitz converse (Ref. [9]) and the Fano inequality (Ref. [2]).

One of their building blocks has been the use of the monotonicity (or data processing inequality) of the divergences in the unified converse. It is interesting to note that a similar approach was followed by Blahut in giving an alternate proof of the Fano inequality in 1976 [25]. This technique was also used by Han and Verdú to generalize the Fano inequality [26].

Instead of relative entropy employed by Blahut, Polyanskiy-Poor-Verdú used generalized divergences that satisfied the monotonicity and other properties. The approach translated the promise of a communication protocol (or a code) of delivering a rate under some fidelity constraints to an upper bound on the fidelity. They also used some derived quantities defined by Csiszár in Ref. [27], who gave their operational characterizations in terms of block coding and hypothesis testing and related it to the Gallager’s error exponent. These quantities play a critical role in the strong converse theorems.

We note that Csiszár’s approach in Ref. [27] was generalized to the quantum domain by Mosonyi and Hiai in Ref. [28] to provide an operational interpretation of the quantum α -relative entropies, but there has been no connection made between the Csiszár’s quantities and the strong converse theorems.

A related work has been the one done by the first author of using monotonicity for proving the generalized quantum Fano inequality in Ref. [29]. Fano inequality is widely used in the converse (not strong) channel capacity theorem proofs. Note that classical Fano inequality has no special relation with the quantum Fano inequality (the former not being a special case of latter) and the technique to generalize the quantum Fano inequality is inherently ‘quantum’ and perhaps the only common thread between the quantum and the classical proof (the latter dating back to Blahut’s work) has been the use of monotonicity.

Our approach in this paper has been to carry this common thread of using monotonicity further and to provide a unified approach to strong converses such as the quantum generalization of the Arimoto’s and Wolfowitz’s with explicit bounds for the latter. We note that no quantum version of Wolfowitz-like bound was known. We build on the above mentioned works in the classical and quantum domains to first list the properties of generalized quantum divergences that we shall need for our proofs. In particular, we show that the quantum Rényi divergences and a non-commutative hockey-stick divergence, that we define, satisfy these properties and suffice to give Arimoto-like bounds with error exponents and also Wolfowitz-like bounds.

We then apply our approach to two quantum channel capacity theorems namely sending classical information across a quantum channel and sending quantum information across a quantum channel. We note that the strong converse for the latter problem has been an open problem for quite sometime.

The organization of the paper is as follows. In Section II, we list the properties we desire from the generalized divergences that can be leveraged for the strong converse theorems. We then derive quantities based on these divergences similar to Csiszár in Ref. [27].

In Section III, we first define the information-processing task for sending the classical information across a quantum channel and then prove a converse for the generalized divergences. We then take specific examples of divergences to yield the two converses - one coinciding with the Ogawa and Nagaoka converse but with an alternate proof and second which is Wolfowitz-like.

In Sec. IV, we repeat the above for sending the quantum information across a quantum channel. The results are quantum error exponent reminiscent of Gallager/Arimoto exponent and then Wolfowitz-like bounds. We give sufficient conditions for the strong converse to hold in general. Lastly, we provide a strong converse for the quantum erasure channel for maximally entangled channel inputs.

The proofs of many Lemmas are given in the Appendix to make the reading of the paper easier. We use the following notation throughout the paper. All the logarithms are natural logarithms. We shall assume that all the quantum systems are finite dimensional. For a given Hilbert space \mathcal{H}_A describing quantum system A , let $\mathcal{S}(\mathcal{H}_A)$ denote the set of all density matrices of \mathcal{H}_A and let $|A|$ be the dimension of \mathcal{H}_A . $\mathbb{1}$ indicates the identity matrix whose dimensions would be clear from the context. For a given square matrix ρ and a scalar x , $\rho + x$ is supposed to mean $\rho + x\mathbb{1}$. A quantum operation is a completely positive and trace preserving (CPTP) map and we use quantum operation, quantum channel, and CPTP map synonymously.

The von Neumann entropy of a quantum state ρ in system A is denoted by $H(A)_\rho$ and if σ^{AB} is a bipartite state in AB , then the quantum mutual information is given by

$$I(A; B)_\sigma := H(A)_\sigma + H(B)_\sigma - H(A, B)_\sigma. \quad (1)$$

The coherent information of σ^{AB} is given by

$$I(A|B)_\sigma := H(B)_\sigma - H(A, B)_\sigma. \quad (2)$$

The projector $P_{\{\rho - \sigma \geq 0\}}$ is a projector onto the positive part of $\rho - \sigma$. For a pure state $|\phi\rangle$, we denote $|\phi\rangle\langle\phi|$ by ϕ . The fidelity between a pure and a mixed state is defined as $F(|\phi\rangle, \rho) = \langle\phi|\rho|\phi\rangle$.

II. GENERALIZED DIVERGENCES

Let us denote a generalized divergence for positive matrices from ρ to σ by $\mathcal{D}(\rho||\sigma)$ that satisfies the following properties:

1. $\mathcal{D}(\rho||\sigma)$ satisfies the monotonicity property (or the data processing inequality), i.e., for any CPTP map \mathcal{E} , we have

$$\mathcal{D}(\rho||\sigma) \geq \mathcal{D}[\mathcal{E}(\rho)||\mathcal{E}(\sigma)]. \quad (3)$$

2. For any quantum state κ ,

$$\mathcal{D}(\rho \otimes \kappa||\sigma \otimes \kappa) = \mathcal{D}(\rho||\sigma). \quad (4)$$

3. Let $\Pi_0 = |0\rangle\langle 0|$ and $\Pi_1 = |1\rangle\langle 1|$ be two projectors with $\Pi_0 + \Pi_1 = \mathbb{1}$.

For $\alpha, \beta \in [0, 1]$, let $\rho = (1 - \alpha)\Pi_0 + \alpha\Pi_1$, $\sigma = \beta\Pi_0 + (1 - \beta)\Pi_1$, and let us define

$$\mathfrak{d}^{(c)}(1 - \alpha||\beta) := \mathcal{D}(\rho||\sigma). \quad (5)$$

Then $\mathfrak{d}^{(c)}(1 - \alpha||\beta)$ is independent of the choice of $\{\Pi_0, \Pi_1\}$ and decreasing for all $\alpha \leq 1 - \beta$.

Let $\alpha \in [0, 1]$, $\beta \in (0, 1]$, $\rho = \alpha\Pi_0 + (1 - \alpha)\Pi_1$, $\sigma = \beta\Pi_0 + (1/\beta - \beta)\Pi_1$, and let us define

$$\mathfrak{d}^{(q)}(\alpha||\beta) := \mathcal{D}(\rho||\sigma). \quad (6)$$

Note that $\sigma \geq 0$ but does not have unit trace. Then $\mathfrak{d}^{(q)}(\alpha||\beta)$ is independent of the choice of $\{\Pi_0, \Pi_1\}$ and increasing for all $\alpha \geq \beta$.

For our purposes, it is not necessary that all these properties are satisfied by a chosen divergence \mathcal{D} . Nevertheless, we give some examples below that satisfy all the above properties.

Some Rényi divergences: For $\rho, \sigma \geq 0$, the Rényi divergence from ρ to σ of order α , $\alpha \in [0, 2] \setminus \{1\}$, is defined as

$$D_\alpha(\rho||\sigma) = \frac{1}{\alpha - 1} \log \text{Tr} \rho^\alpha \sigma^{1-\alpha} \quad (7)$$

and limit is taken at $\alpha = 1$. The monotonicity property is proved in Ref. [30] (see Example 4.5) and the other properties are not difficult to show.

Non-commutative hockey-stick divergence: It has been shown in Refs. [23, 24] that the classical Wolfowitz converse giving explicit bounds can be obtained using the f -divergence with

$$f(x) = (x - \gamma)^+, \quad (8)$$

where $x^+ = x$ if $x > 0$ and 0 otherwise. This function is known as the hockey-stick function and has applications in finance [31]. It might be tempting to define a quantum f -divergence (see Refs. [30, 32, 33]) using $f(x)$ but $f(x)$ is not operator convex [34] and operator convexity is typically used for proving the monotonicity property. However, there is a workaround. Let the Jordan decomposition of a square matrix κ be given by $\kappa = \kappa^+ - \kappa^-$, where κ^+ and κ^- are the positive and the negative parts of κ . Then we could define the non-commutative hockey-stick divergence (or simply hockey-stick divergence) as

$$\mathcal{D}(\rho||\sigma) = \text{Tr}(\rho - \gamma\sigma)^+, \quad (9)$$

where $\gamma \geq 1$. Note that this is not a f -divergence in the sense of [30, 32, 33]. In fact, it is related to the trace distance since $2(x - \gamma)^+ = |x - \gamma| + (x - \gamma)$, and hence, for quantum states ρ and σ , we have

$$2\mathcal{D}(\rho||\sigma) = \text{Tr}|\rho - \gamma\sigma| + \text{Tr}(\rho - \gamma\sigma) \quad (10)$$

$$= \|\rho - \gamma\sigma\|_1 + (1 - \gamma). \quad (11)$$

The monotonicity follows from Lemma 4 in the Appendix and the other properties are not difficult to show.

A. Derived quantities

We now define two quantities for bipartite states $\rho^{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ derived from the generalized divergence $\mathcal{D}(\cdot||\cdot)$ as

$$\mathcal{K}^{(c)}(A; B)_\rho := \inf_{\sigma^B \in \mathcal{S}(\mathcal{H}_B)} \mathcal{D}(\rho^{AB}||\rho^A \otimes \sigma^B), \quad (12)$$

$$\mathcal{K}^{(q)}(A; B)_\rho := \inf_{\sigma^B \in \mathcal{S}(\mathcal{H}_B)} \mathcal{D}(\rho^{AB}||\mathbb{1} \otimes \sigma^B), \quad (13)$$

where $\rho^A = \text{Tr}_B \rho^{AB}$. We now have the following lemma that shows that both the above derived quantities satisfy the data processing inequality.

Lemma 1. *Let $\mathcal{E}^{B \rightarrow C}$ be a CPTP map and $\rho^{AC} = \mathcal{E}^{B \rightarrow C}(\rho^{AB})$. Then*

$$\mathcal{K}^{(c)}(A; B)_\rho \geq \mathcal{K}^{(c)}(A; C)_\rho, \quad (14)$$

$$\mathcal{K}^{(q)}(A; B)_\rho \geq \mathcal{K}^{(q)}(A; C)_\rho. \quad (15)$$

Let $\rho^{ABC} = \rho^{AB} \otimes \rho^C$. Then

$$\mathcal{K}^{(c)}(A; B)_\rho \geq \mathcal{K}^{(c)}(A; BC)_\rho. \quad (16)$$

Proof. For any $\delta > 0$, there exists a σ^B such that $\mathcal{K}^{(c)}(A; B)_\rho \geq \mathcal{D}(\rho^{AB} \| \rho^A \otimes \sigma^B) - \delta$. We now have

$$\mathcal{K}^{(c)}(A; B)_\rho \geq \mathcal{D}(\rho^{AB} \| \rho^A \otimes \sigma^B) - \delta \quad (17)$$

$$\geq \mathcal{D}[\rho^{AC} \| \rho^A \otimes \mathcal{E}^{B \rightarrow C}(\sigma^B)] - \delta \quad (18)$$

$$\geq \inf_{\sigma^C} \mathcal{D}(\rho^{AC} \| \rho^A \otimes \sigma^C) - \delta \quad (19)$$

$$= \mathcal{K}^{(c)}(A; C)_\rho - \delta. \quad (20)$$

Since this is true for any $\delta > 0$, the result follows. The proof of (15) is similar and we omit it. To show (16), note that

$$\mathcal{K}^{(c)}(A; B)_\rho = \inf_{\sigma^B} \mathcal{D}(\rho^{AB} \| \rho^A \otimes \sigma^B) \quad (21)$$

$$= \inf_{\sigma^B} \mathcal{D}(\rho^{AB} \otimes \rho^C \| \rho^A \otimes \sigma^B \otimes \rho^C) \quad (22)$$

$$= \inf_{\sigma^B} \mathcal{D}(\rho^{ABC} \| \rho^A \otimes \sigma^B \otimes \rho^C) \quad (23)$$

$$\geq \inf_{\sigma^{BC}} \mathcal{D}(\rho^{ABC} \| \rho^A \otimes \sigma^{BC}) \quad (24)$$

$$= \mathcal{K}^{(c)}(A; BC)_\rho. \quad (25)$$

QED. □

Note that the above definition of $\mathcal{K}^{(c)}$ can be easily extended for the classical random variables by assuming that the density matrices are commuting and the random variables have probability distributions given by the eigenvalues. This definition would be the same as the one in Ref. [24] given by

$$\mathcal{K}^{(c)}(X; Y) = \inf_{Q_Y \in \mathcal{P}_Y} \mathcal{D}(P_{XY} \| P_X \times Q_Y), \quad (26)$$

where P_{XY} is the joint probability distribution of the pair of random variables (X, Y) , P_X is the probability distribution of X that can be deduced from P_{XY} , and \mathcal{P}_Y is the set of all probability distributions that Y can take. The following result will be useful later.

Lemma 2 (Polyanskiy and Verdú, 2010 [24]). *Let the random variables S, X, Y, \hat{S} form a Markov chain $S - X - Y - \hat{S}$. Then*

$$\mathcal{K}^{(c)}(S; \hat{S}) \leq \mathcal{K}^{(c)}(X; Y). \quad (27)$$

III. CLASSICAL INFORMATION OVER QUANTUM CHANNEL

A. Information processing task and converse

For a given message source and a communication channel, a communication protocol consists of an encoder and decoder entrusted with the task of replicating the message at the receiver within some prescribed error.

Suppose Alice wants to send classical information to Bob using a quantum channel. We model the information as a uniformly distributed random variable S that takes values over the set $\{1, 2, \dots, e^{n\mathcal{R}}\}$. Alice maps S to X using, possibly, a randomized encoder modeled by the conditional probability distribution $P_{X|S}$, where X takes values over $\{1, 2, \dots, |\mathcal{X}|\}$. The encoder's output is then mapped to $\rho_X^{A'n} \in \mathcal{S}(\mathcal{H}_{A'^n})$ and is sent to Bob over n independent uses of the channel $\mathcal{N}^{A' \rightarrow B}$. It is useful to represent the state of input to the channel as a cq (classical-quantum) state given by

$$\rho^{MA'^n} = \sum_x P_X(x) |x\rangle\langle x|^M \otimes \rho_x^{A'^n}. \quad (28)$$

Bob receives his part, B^n , of

$$\rho^{MB^n} = \mathcal{N}^{A'^n \rightarrow B^n}(\rho^{MA'^n}), \quad (29)$$

where $\mathcal{N}^{A'^n \rightarrow B^n} = \left(\mathcal{N}^{A' \rightarrow B}\right)^{\otimes n}$, and to find out the classical message that Alice sent for him, Bob applies a POVM $\{\Lambda_y^{B^n}\}$, $y \in \{1, 2, \dots, |\mathcal{Y}|\}$, and the outcome of the measurement process is modeled by a random variable Y where

$$P_{Y|X}(y|x) = \Pr\{Y = y|X = x\} = \text{Tr} \Lambda_y^{B^n} \left(\mathcal{N}^{A' \rightarrow B}\right)^{\otimes n} \rho_x^{A'^n}. \quad (30)$$

The random variable Y is then further processed (decoded) by Bob to yield \hat{S} as an estimate of the message S . The average probability of error is given by $\Pr\{S \neq \hat{S}\}$.

If the above communication protocol achieves an average probability of error not larger than ε , then we shall refer to such a protocol as a $(n, \mathcal{R}, \varepsilon)$ code.

We first prove an inequality similar to the Holevo bound for $\mathcal{K}^{(c)}$.

Lemma 3 (Holevo-like bound for $\mathcal{K}^{(c)}$). *For any n and any POVM $\{\Lambda_y^{B^n}\}$, we have*

$$\mathcal{K}^{(c)}(X; Y) \leq \mathcal{K}^{(c)}(M; B^n)_\rho. \quad (31)$$

Proof. We prove it for $n = 1$ and the extension to any n is straightforward. Consider an ancilla quantum system C that is uncorrelated with the system MB and the joint state of MBC is given by

$$\rho^{MBC} = \sum_x P_X(x) |x\rangle\langle x|^M \otimes \mathcal{N}^{A' \rightarrow B}(\rho_X^{A'}) \otimes |1\rangle\langle 1|^C, \quad (32)$$

where $\{|i\rangle^C\}$, $i = 1, 2, \dots, |C|$ is an orthonormal basis in \mathcal{H}_C . Let $\mathcal{E}^{BC \rightarrow B'C'}$ be a CPTP map with Krauss operators $\{\sqrt{\Lambda_y} \otimes U_y\}$, $y = 1, 2, \dots, |\mathcal{Y}|$, where U_y is a Unitary matrix such that $U_y|1\rangle^C = |y\rangle^C$. The state after applying the map $\mathcal{E}^{BC \rightarrow B'C'}$ is given by

$$\rho^{MB'C'} = \sum_{x,y} P_X(x) |x\rangle\langle x|^M \otimes \sqrt{\Lambda_y} \mathcal{N}^{A' \rightarrow B}(\rho_X^{A'}) \sqrt{\Lambda_y} \otimes |y\rangle\langle y|^C. \quad (33)$$

We now have the following inequalities

$$\mathcal{K}^{(c)}(M; B)_\rho \stackrel{a}{\geq} \mathcal{K}^{(c)}(M; BC)_\rho \quad (34)$$

$$\geq \mathcal{K}^{(c)}(M; B'C')_\rho \quad (35)$$

$$\geq \mathcal{K}^{(c)}(M; C')_\rho, \quad (36)$$

where a follows from (16). Note that

$$\rho^{MC'} = \sum_{x,y} P_X(x) P_{Y|X}(y|x) |x\rangle\langle x|^M \otimes |y\rangle\langle y|^C. \quad (37)$$

Let $\Pi_y = |y\rangle\langle y|^C$ and let us define a quantum operation \mathcal{F} on the system C' with Krauss operators $\{\Pi_y\}$. Since $\mathcal{F}^{C' \rightarrow C''}(\rho^{MC'}) = \rho^{MC'}$, hence, using the data processing inequality, for any $\sigma^{C'} \in \mathcal{S}(\mathcal{H}_{C'})$, we get

$$\mathcal{D}(\rho^{MC'} \parallel \rho^M \otimes \sigma^{C'}) \geq \mathcal{D}[\rho^{MC'} \parallel \rho^M \otimes \mathcal{F}^{C' \rightarrow C''}(\sigma^{C'})]. \quad (38)$$

This indicates that for the minimization, one may consider only those $\sigma^{C'}$ that have $\{|y\rangle^C\}$ as the eigenvectors which would lead us to the classical divergence in (26) and hence,

$$\mathcal{K}^{(c)}(M; C')_\rho = \mathcal{K}^{(c)}(X; Y). \quad (39)$$

QED. □

We now prove a theorem that would allow us to yield the various converses.

Theorem 1. For $\varepsilon \leq 1 - e^{-n\mathcal{R}}$, any $(n, \mathcal{R}, \varepsilon)$ code satisfies

$$\mathcal{d}^{(c)}(1 - \varepsilon \parallel e^{-n\mathcal{R}}) \leq \mathcal{K}^{(c)}(M; B^n)_\rho. \quad (40)$$

Proof. We have the following inequalities

$$\mathcal{K}^{(c)}(M; B^n)_\rho \stackrel{a}{\geq} \mathcal{K}^{(c)}(X; Y) \quad (41)$$

$$\stackrel{b}{\geq} \mathcal{K}^{(c)}(S; \hat{S}) \quad (42)$$

$$\stackrel{c}{\geq} \mathcal{d}^{(c)}(\Pr\{S = \hat{S}\} \parallel e^{-n\mathcal{R}}) \quad (43)$$

$$\stackrel{d}{\geq} \mathcal{d}^{(c)}(1 - \varepsilon \parallel e^{-n\mathcal{R}}), \quad (44)$$

where a follows from Lemma 3, b follows from Lemma 2, c follows by applying the classical transformation $(S, \hat{S}) \rightarrow \delta_{S, \hat{S}}$, where $\delta_{x,y} = 1$ if $x = y$ and 0 otherwise, and d follows from Property 3 in Sec. II pertaining to $\mathcal{d}^{(c)}$. □

It may be worth mentioning that the constraint $\varepsilon \leq 1 - e^{-n\mathcal{R}}$ may not be seen as weakening the strong converse because, if the constraint is violated, i.e., $\varepsilon \geq 1 - e^{-n\mathcal{R}}$, then it, by itself, would imply an exponential convergence of ε to 1, where \mathcal{R} is bounded from below (since we are proving the converse) by the channel capacity.

We are now in a position to apply Theorem 1 to yield the various converses.

B. New proof of the Ogawa and Nagaoka converse

We assume that $n = 1$ which is clearly the most general case. Take \mathcal{D} to be D_λ , the Rényi divergence of order $\lambda \in [0, 2] \setminus \{1\}$, in Theorem 1 to get

$$\mathfrak{d}^{(c)}(1 - \varepsilon || e^{-\mathcal{R}}) \leq \inf_{\sigma^B \in \mathcal{S}(\mathcal{H}_B)} D_\lambda(\rho^{MB} || \rho^M \otimes \sigma^B). \quad (45)$$

For a cq-state ρ^{MB} , we note from Ref. [17] that

$$D_\lambda(\rho^{MB} || \rho^M \otimes \sigma^B) = D_\lambda(\rho^{MB} || \rho^M \otimes \sigma^*) + D_\lambda(\sigma^* || \sigma^B), \quad (46)$$

where

$$\sigma^* = \frac{\xi^B}{\text{Tr} \xi^B}, \quad \text{with} \quad \xi^B = \left(\sum_x P_X(x) \rho_x^B \right)^\lambda. \quad (47)$$

Hence, the minimum of the RHS of (45) is achieved at $\sigma^B = \sigma^*$. Substituting in (45), we get

$$\mathfrak{d}^{(c)}(1 - \varepsilon || e^{-\mathcal{R}}) \leq \frac{\lambda}{1 - \lambda} E_0(s, \mathcal{N}^{A' \rightarrow B})_{\{P_X(x), \rho_x^{A'}\}}, \quad (48)$$

where

$$E_0(s, \mathcal{N}^{A' \rightarrow B})_{\{P_X(x), \rho_x^{A'}\}} = -\log \text{Tr} \left\{ \sum_x P_X(x) \left[\mathcal{N}^{A' \rightarrow B}(\rho_x^{A'}) \right]^{1/(s+1)} \right\}^{s+1}. \quad (49)$$

Using the inequality

$$\mathfrak{d}^{(c)}(1 - \varepsilon || e^{-\mathcal{R}}) \geq \frac{\lambda}{\lambda - 1} \log(1 - \varepsilon) + \mathcal{R}, \quad (50)$$

we get for $\lambda \in (1, 2]$, $s = \lambda^{-1} - 1$ and hence, $s \in [-1/2, 0)$ that

$$\varepsilon > 1 - \exp \left\{ - \left[-s\mathcal{R} + E_0(s, \mathcal{N}^{A' \rightarrow B})_{\{P_X(x), \rho_x^{A'}\}} \right] \right\}, \quad (51)$$

The rest of the treatment is the same as in Ref. [16]. For a $(n, \mathcal{R}, \varepsilon)$ code, let Alice send unentangled inputs across the channel uses, i.e., the ensemble across the n channel uses is given by

$$\left\{ \prod_{i=1}^n P_X(x_i), \bigotimes_{i=1}^n \mathcal{N}^{A'_i \rightarrow B_i}(\rho_{x_i}^{A'_i}) \right\}, \quad x_i \in \{1, 2, \dots, |\mathcal{X}|\}, \quad \forall i. \quad (52)$$

Theorem 2. For a $(n, \mathcal{R}, \varepsilon)$ code and for all $n \in \mathbb{N}$ with unentangled inputs, the following lower bound holds

$$\varepsilon \geq 1 - \exp \left\{ -n \left[-s\mathcal{R} + E_0(s, \mathcal{N}^{A' \rightarrow B})_{\{P_X(x), \rho_x^{A'}\}} \right] \right\}. \quad (53)$$

It is also shown in Ref. [16] and not too difficult to check that

$$\left. \frac{\partial E_0(s, \mathcal{N}^{A' \rightarrow B})_{\{P_X(x), \rho_x^{A'}\}}}{\partial s} \right|_{s=0} = I(M; B)_\rho, \quad (54)$$

and if $\mathcal{R} > C^{(1)}(\mathcal{N})$ [35], where

$$C^{(1)}(\mathcal{N}) = \max_{\{P_X(x), \rho_x^{A'}\}} I(M; B)_\rho, \quad (55)$$

then $\exists t \in [-1/2, 0)$ such that $\forall s \in (-t, 0)$,

$$-s\mathcal{R} + E_0(s, \mathcal{N}^{A' \rightarrow B})_{\{P_X(x), \rho_x^{A'}\}} > 0. \quad (56)$$

Hence, it implies using (53) that the probability of error approaches 1 exponentially.

Note that we had to confine s in $[-1/2, 0)$ instead of $[-1, 0)$ since the monotonicity of quantum Rényi divergence of order λ is known to hold for $\lambda \in [0, 2]$ [28, 30]. This does not, however, affect the strong converse proof since the Lemma 3 in Ref. [16] would still hold.

C. Wolfowitz converse

Again, we first assume $n = 1$ before going to any n . Take \mathcal{D} to be the hockey-stick divergence. We first note that

$$\mathcal{D}^{(c)}(1 - \varepsilon || e^{-\mathcal{R}}) = (1 - \varepsilon - \gamma e^{-\mathcal{R}})^+ + [\varepsilon - \gamma(1 - e^{-\mathcal{R}})]^+ \quad (57)$$

$$\geq 1 - \varepsilon - \gamma e^{-\mathcal{R}} \quad (58)$$

and hence, using Theorem 1, we have

$$\varepsilon \geq 1 - \mathcal{K}^{(c)}(M; B)_\rho - \gamma e^{-\mathcal{R}}. \quad (59)$$

Note that

$$\mathcal{K}^{(c)}(M; B)_\rho \leq \text{Tr} P_{\{\rho^{MB} - \gamma \rho^M \otimes \rho^B > 0\}} \rho^{MB}. \quad (60)$$

We now give an upper bound for the RHS of the above equation that is reminiscent of the Chebyshev's inequality in the classical setting. Using Lemma 6, we get for $\log \gamma > I(M; B)_\rho$,

$$\text{Tr} P_{\{\rho^{MB} - \gamma \rho^M \otimes \rho^B > 0\}} \rho^{MB} \leq \frac{\text{Tr} \rho^{MB} [\log \rho^{MB} - \log(\rho^M \otimes \rho^B)]^2 - [I(M; B)_\rho]^2}{[\log \gamma - I(M; B)_\rho]^2}, \quad (61)$$

Define for any $n \in \mathbb{N}$,

$$\mathcal{A}_n^{(c)} := \max_{\rho^{MA^n}} \left\{ \text{Tr} \rho^{MB^n} [\log \rho^{MB^n} - \log(\rho^M \otimes \rho^{B^n})]^2 - [I(M; B^n)_\rho]^2 \right\}. \quad (62)$$

This quantity (without the maximization over the channel input) has been known in the classical case as the information variance and was defined by Shannon (see Ref. [23] for more details). The finiteness of $\mathcal{A}_1^{(c)}$ follows from Lemma 9. Using Theorem 1, (58) and (61), we get

$$\varepsilon \geq 1 - \frac{\mathcal{A}_1^{(c)}}{[\log \gamma - I(M; B)_\rho]^2} - \gamma e^{-\mathcal{R}}. \quad (63)$$

For a $(n, \mathcal{R}, \varepsilon)$ code and unentangled inputs described in (52), it is not difficult to show that $\mathcal{A}_n^{(c)} = n\mathcal{A}_1^{(c)}$. Then choosing $\log \gamma = nC^{(1)}(\mathcal{N}) + n\delta$ for some $\delta > 0$, where $C^{(1)}(\mathcal{N})$ is defined in (55), we get for this $(n, \mathcal{R}, \varepsilon)$ code

$$\varepsilon \geq 1 - \frac{\mathcal{A}_1^{(c)}}{n\delta^2} - e^{-n[\mathcal{R} - C^{(1)}(\mathcal{N}) - \delta]}. \quad (64)$$

Choosing $\delta = [\mathcal{R} - C^{(1)}(\mathcal{N})]/2$, we get the following result.

Theorem 3. *For a $(n, \mathcal{R}, \varepsilon)$ code with the ensemble given in (52), the following lower bound holds*

$$\varepsilon \geq 1 - \frac{4\mathcal{A}_1^{(c)}}{n[\mathcal{R} - C^{(1)}(\mathcal{N})]^2} - e^{-n[\mathcal{R} - C^{(1)}(\mathcal{N})]/2}. \quad (65)$$

Note that (65) has the same form as the classical Wolfowitz strong converse (see Ref. [7]).

IV. QUANTUM INFORMATION OVER QUANTUM CHANNEL

A. Information processing task and converse

Suppose a quantum system S and a reference system A have a state $|\phi\rangle^{AS}$. Alice only has access to the system S and not to A . Alice wants to send her part of the shared state with A to Bob using n independent uses of a quantum channel $\mathcal{N}^{A' \rightarrow B}$ such that at the end of the communication protocol chain, Bob's shared state with the reference A is arbitrarily close to the state Alice shared with A . We shall call \mathcal{R} to be the communication rate and is given by

$$\mathcal{R} := \frac{\log |S|}{n}. \quad (66)$$

We shall assume that the state of S is given by $e^{-n\mathcal{R}} \mathbb{1}$, i.e., a completely mixed state.

To this end, Alice performs an encoding operation given by $\mathcal{E}^{S \rightarrow A'^n}$ to get

$$\rho^{AA'^n} = \mathcal{E}^{S \rightarrow A'^n} (\phi^{AS}). \quad (67)$$

Alice transmits the system A'^n over $\mathcal{N}^{A'^n \rightarrow B^n} = \left(\mathcal{N}^{A' \rightarrow B}\right)^{\otimes n}$ and Bob receives the state

$$\rho^{AB^n} = \mathcal{N}^{A'^n \rightarrow B^n} \left[\mathcal{E}^{S \rightarrow A'^n} (\phi^{AS}) \right]. \quad (68)$$

Bob applies a decoding operation on its part of the received state to get

$$\rho^{A\hat{S}} = \mathcal{T}^{B^n \rightarrow \hat{S}} \left\{ \mathcal{N}^{A'^n \rightarrow B^n} \left[\mathcal{E}^{S \rightarrow A'^n} (\phi^{AS}) \right] \right\}. \quad (69)$$

The performance of the protocol is quantified by the fidelity given by

$$F(\phi^{AS}, \rho^{A\hat{S}}) = \langle \phi |^{AS} \rho^{A\hat{S}} | \phi \rangle^{AS}. \quad (70)$$

If we are given that the protocol achieves a fidelity not smaller than \mathbb{F} , then we shall refer to such a protocol as a $(n, \mathcal{R}, 1 - \mathbb{F})$ code.

The maximum rate per channel use for this protocol in the limit of large number of channel uses and fidelity arbitrarily close to 1 was proved in a series of papers [36–43]. Let the coherent information of the channel $\mathcal{N}^{A' \rightarrow B}$ be defined as

$$Q(\mathcal{N}) := \max_{\rho^{AA'}} I(A)B)_\sigma, \quad (71)$$

where $\sigma^{AB} = \mathcal{N}^{A' \rightarrow B}(\rho^{AA'})$. The capacity of the channel is now given by the regularization

$$Q_{\text{reg}}(\mathcal{N}) := \lim_{n \rightarrow \infty} \frac{Q(\mathcal{N}^{\otimes n})}{n}. \quad (72)$$

We now prove a theorem that would give us one-shot inequalities between the fidelity and the rate.

Theorem 4. For $\mathbb{F} \geq e^{-n\mathcal{R}}$, any $(n, \mathcal{R}, 1 - \mathbb{F})$ code satisfies

$$\mathfrak{d}^{(q)}(\mathbb{F} || e^{-n\mathcal{R}}) \leq \mathcal{K}^{(q)}(A; B^n)_\rho. \quad (73)$$

Proof. Let $\{|i\rangle^{AS}\}$ be an orthonormal basis for \mathcal{H}_{AS} with $|1\rangle^{AS} = |\phi\rangle^{AS}$. Consider a CPTP quantum map $\mathcal{F}^{A\hat{S} \rightarrow C}$ where $|C| = 2$ with Krauss operators $|0\rangle^C \langle 1|^{AS}$, and $\{|1\rangle^C \langle i|^{AS}\}$, $i = 2, 3, \dots, |AS|$. Let $\Pi_0^C = 0^C$ and $\Pi_1^C = 1^C$. Then we have

$$\mathcal{F}(\rho^{A\hat{S}}) = \mathbb{F}' \Pi_0^C + (1 - \mathbb{F}') \Pi_1^C, \quad (74)$$

$$\mathcal{F}(\mathbb{1} \otimes \sigma^{\hat{S}}) = e^{-n\mathcal{R}} \Pi_0^C + (e^{n\mathcal{R}} - e^{-n\mathcal{R}}) \Pi_1^C, \quad (75)$$

where $\mathbb{F}' = \langle \phi |^{AS} \rho^{A\hat{S}} | \phi \rangle^{AS}$ and (75) holds for all quantum states $\sigma^{\hat{S}}$. We now have the following inequalities

$$\mathcal{K}^{(q)}(A; B^n)_\rho \stackrel{a}{\geq} \mathcal{K}^{(q)}(A; \hat{S})_\rho \quad (76)$$

$$= \inf_{\sigma^{\hat{S}}} \mathcal{D}(\rho^{A\hat{S}} || \mathbb{1} \otimes \sigma^{\hat{S}}) \quad (77)$$

$$\stackrel{b}{\geq} \inf_{\sigma^{\hat{S}}} \mathcal{D}[\mathbb{F}' \Pi_0^C + (1 - \mathbb{F}') \Pi_1^C || e^{-n\mathcal{R}} \Pi_0^C + (e^{n\mathcal{R}} - e^{-n\mathcal{R}}) \Pi_1^C] \quad (78)$$

$$\stackrel{c}{=} \mathfrak{d}^{(q)}(\mathbb{F}' || e^{-n\mathcal{R}}) \quad (79)$$

$$\stackrel{d}{\geq} \mathfrak{d}^{(q)}(\mathbb{F} || e^{-n\mathcal{R}}), \quad (80)$$

where a and b follow from the data processing inequality, c follows since the quantity $\mathfrak{d}^{(q)}(\mathbb{F}' || e^{-n\mathcal{R}})$ is independent of $\sigma^{\hat{S}}$, and d from Property 3 in Sec. II pertaining to $\mathfrak{d}^{(q)}$. \square

We now give upper bounds to the fidelity using the Rényi and the hockey-stick divergences.

B. Quantum Error exponent

Let us first assume that $n = 1$. Take \mathcal{D} to be the Rényi divergence of order $\lambda \in [0, 2] \setminus \{1\}$. We first note that

$$\mathfrak{d}^{(q)}(\mathbb{F} || e^{-\mathcal{R}}) \geq \frac{\lambda}{\lambda - 1} \log \mathbb{F} + \mathcal{R} \quad (81)$$

and it follows from Lemma 7 that

$$\mathcal{K}^{(q)}(A; B)_\rho = \frac{\lambda}{1 - \lambda} E_0(\lambda^{-1} - 1, \mathcal{N}^{A' \rightarrow B})_\rho, \quad (82)$$

where for $s = \lambda^{-1} - 1$, $s \in [-1/2, 0)$,

$$E_0(s, \mathcal{N}^{A' \rightarrow B})_\rho := -\log \text{Tr} \left\{ \text{Tr}_A \left[\mathcal{N}^{A' \rightarrow B}(\rho^{AA'}) \right]^{1/(1+s)} \right\}^{s+1}, \quad (83)$$

whose properties are studied by the following theorem.

Theorem 5. *For any quantum state σ^{AB} , the function*

$$g(s) := -\log \text{Tr} \left[\text{Tr}_A (\sigma^{AB})^{1/(1+s)} \right]^{s+1}, \quad s \in [-1/2, 0), \quad (84)$$

satisfies

$$g(0) = 0, \quad (85)$$

$$\left. \frac{\partial g(s)}{\partial s} \right|_{s=0} = I(A; B)_\sigma, \quad (86)$$

and $g(s) + (s + 1) \log |A|$ is an increasing function in s .

Proof. See appendix. □

Using (73), we get the one-shot bound on the fidelity as

$$\mathbb{F} \leq \exp \left\{ - \left[-s\mathcal{R} + E_0(s, \mathcal{N}^{A' \rightarrow B})_\rho \right] \right\}. \quad (87)$$

One could provide a sufficient condition for the strong converse to exist as an additivity question. First define

$$E_0^*(s, \mathcal{N}) := \min_{\rho^{AA'}} E_0(s, \mathcal{N})_\rho, \quad (88)$$

where we just abbreviate \mathcal{N} for $\mathcal{N}^{A' \rightarrow B}$. Then one could make the following statement. For $\mathcal{R} \geq Q_{\text{reg}}(\mathcal{N})$, strong converse holds for all inputs if for all $m, n \in \mathbb{N} \exists t \in [-\frac{1}{2}, 0)$ such that $\forall s \in (t, 0)$,

$$E_0^*(s, \mathcal{N}^{\otimes n+m}) = E_0^*(s, \mathcal{N}^{\otimes n}) + E_0^*(s, \mathcal{N}^{\otimes m}). \quad (89)$$

This statement is easy to prove. Using (87), we have

$$\mathbb{F} \leq \exp \left\{ -n \left[-s\mathcal{R} + \frac{E_0^*(s, \mathcal{N}^{\otimes n})_\rho}{n} \right] \right\}. \quad (90)$$

If (89) is satisfied, then $\forall s \in (t, 0)$,

$$\frac{E_0^*(s, \mathcal{N}^{\otimes n})_\rho}{n} = E_0^*(s, \mathcal{N})_\rho. \quad (91)$$

It follows from Lemma 8 that $\exists t' \in [-\frac{1}{2}, 0)$ such that $\forall s \in (t', 0)$, $-s\mathcal{R} + E_0^*(s, \mathcal{N})_\rho > 0$. Hence $\forall s \in (\max\{t, t'\}, 0)$ and $\forall n$,

$$-s\mathcal{R} + \frac{E_0^*(s, \mathcal{N}^{\otimes n})_\rho}{n} > 0 \quad (92)$$

and is independent of n . (89) is unlikely to hold in general. Observe that if the dimension of the quantum system A is not constraining, then (89) implies the additivity of the coherent information of the channel. To see this, divide (89) by s and take the limit $s \uparrow 0$, invoke Theorem 5 and since $s < 0$, the minimum would be replaced by maximum over the input states. It would be interesting to find out if there is a class of channels for which (89) holds.

C. Wolfowitz converse

Take \mathcal{D} to be the hockey-stick divergence. Following the same steps as in III C, we get for $n = 1$

$$\mathfrak{d}^{(q)}(\mathbb{F} || e^{-\mathcal{R}}) \geq \mathbb{F} - \gamma e^{-\mathcal{R}}, \quad (93)$$

$$\mathcal{K}^{(q)}(A; B)_\rho \leq \text{Tr} P_{\{\rho^{AB} - \gamma \mathbb{1} \otimes \rho^B > 0\}} \rho^{AB}. \quad (94)$$

We upper bound the RHS of the above equation using Lemma 6, for $\log \gamma > I(A)B)_\rho$ as

$$\text{Tr} P_{\{\rho^{AB} - \gamma \mathbb{1} \otimes \rho^B > 0\}} \rho^{AB} \leq \frac{\text{Tr} \rho^{AB} [\log \rho^{AB} - \log(\mathbb{1} \otimes \rho^B)]^2 - [I(A)B)_\rho]^2}{[\log \gamma - I(A)B)_\rho]^2}, \quad (95)$$

we get

$$\mathbb{F} \leq \frac{\mathcal{A}_1^{(q)}}{[\log \gamma - I(A)B)_\rho]^2} + \gamma e^{-\mathcal{R}}, \quad (96)$$

where

$$\mathcal{A}_n^{(q)} = \max_{\rho^{AA^n}} \left\{ \text{Tr} \rho^{AB^n} [\log \rho^{AB^n} - \log(\mathbb{1} \otimes \rho^{B^n})]^2 - [I(A)B^n)_\rho]^2 \right\}. \quad (97)$$

For a $(n, \mathcal{R}, 1 - \mathbb{F})$ code, choosing $\log \gamma = nQ_{\text{reg}}(\mathcal{N}) + n\delta$ for some $\delta > 0$, we get an upper bound

$$\mathbb{F} \leq \frac{\mathcal{A}_n^{(q)}}{n^2 \delta^2} + \exp \{-n[\mathcal{R} - Q_{\text{reg}}(\mathcal{N}) - \delta]\}. \quad (98)$$

Choosing $\delta = [\mathcal{R} - Q_{\text{reg}}(\mathcal{N})]/2$, we get

$$\mathbb{F} \leq \frac{4\mathcal{A}_n^{(q)}}{n^2 [\mathcal{R} - Q_{\text{reg}}(\mathcal{N})]^2} + \exp \left\{ -\frac{n}{2} [\mathcal{R} - Q_{\text{reg}}(\mathcal{N})] \right\}. \quad (99)$$

Hence, a sufficient condition for the strong converse to hold is that $\mathcal{A}_n^{(q)}/n^2 \rightarrow 0$ as $n \rightarrow \infty$.

D. Strong converse for the quantum erasure channel for maximally entangled channel inputs

A quantum erasure channel $\mathcal{N}_p^{A' \rightarrow B}$, defined in Ref. [44], is given by the following Krauss operators $\left\{ \sqrt{(1-p)} |i\rangle^B \langle i|^{A'}, \sqrt{p} |e\rangle^B \langle i|^{A'} \right\}, i = 1, \dots, |A'|, p \in [0, 1], |B| = |A'| + 1, \left\{ |i\rangle^{A'} \right\}, \left\{ |i\rangle^B \right\}$ are orthonormal basis in $\mathcal{H}_{A'}$ and \mathcal{H}_B respectively, and $|e\rangle^B = |j\rangle^B$ for $j = |B|$. The action of the channel can be understood as follows

$$\mathcal{N}_p^{A' \rightarrow B}(\rho^{AA'}) = (1-p)\sigma^{AB} + p\rho^A \otimes |e\rangle\langle e|^B. \quad (100)$$

Let $\sigma^{AB} = \mathcal{G}^{A' \rightarrow B}(\rho^{AA'})$, where \mathcal{G} increases the dimension but leaves the state intact. Then with probability $1-p$, the channel leaves the state as σ^{AB} and with probability p it erases the state and replaces by $|e\rangle^B$. It is not difficult to see that σ^{AB} is orthogonal to $\rho^A \otimes |e\rangle\langle e|^B$.

One could carry over this observation for 2 channel uses. Let $\sigma^{AB^2} = (\mathcal{G}^{A' \rightarrow B})^{\otimes 2}(\rho^{AA'^2})$. Observe that

$$\begin{aligned} \left(\mathcal{N}_p^{A'_1 \rightarrow B_1} \otimes \mathcal{N}_p^{A'_2 \rightarrow B_2} \right) (\rho^{AA'_1 A'_2}) &= (1-p)^2 \sigma^{AB_1 B_2} + p(1-p) \sigma^{AB_1} \otimes |e\rangle\langle e|^{B_2} \\ &\quad + p(1-p) \sigma^{AB_2} \otimes |e\rangle\langle e|^{B_1} + p^2 \rho^A \otimes |e\rangle\langle e|^{B_1} \otimes |e\rangle\langle e|^{B_2}, \end{aligned} \quad (101)$$

where we use the usual notation for the reduced density matrices, i.e., for example, representing σ^{AB_1} as the result of partial trace over B_2 of σ^{AB^2} , each of these four matrices are orthogonal to each other and we have an abuse of notation in the third term by rearranging the order of the systems.

Taking this further for n channel uses, let $\sigma^{AB^n} = (\mathcal{G}^{A' \rightarrow B})^{\otimes n}(\rho^{AA'^n})$. The output can be written as the sum of 2^n orthogonal density matrices where each of these matrices results from i erasures $i \in \{0, \dots, n\}$ and this occurs with probability $(1-p)^{n-i} p^i$. The number of states that have suffered exactly i erasures is $\binom{n}{i}$.

Let $B_{i_1} B_{i_2} \dots B_{i_{n-k}}$ be the quantum systems that have not suffered erasures and we could write the state in this case using σ^{AB^n} as

$$\zeta_{i_1, \dots, i_{n-k}}^{AB_{i_1} B_{i_2} \dots B_{i_n}} = \sigma^{AB_{i_1} B_{i_2} \dots B_{i_{n-k}}} \otimes \bigotimes_{j=1}^k |e\rangle\langle e|^{B_{i_{n-k+j}}}. \quad (102)$$

It now follows that

$$\rho^{AB^n} = \sum_{2^n \text{ terms}} \alpha_{k,n} \times \zeta_{i_1, \dots, i_{n-k}}^{AB_{i_1} B_{i_2} \dots B_{i_n}}, \quad (103)$$

where

$$\alpha_{k,n} = (1-p)^{n-k} p^k. \quad (104)$$

To prove the strong converse, we find an upper bound for $\mathcal{K}^{(q)}(A; B^n)$. We assume that $\rho^{AA'^n}$ is a maximally entangled state with a Schmidt rank of $|A|$. Let the channel input be d_A dimensional and for n channel uses, $|A| = d_A^n$. It is known that $Q(\mathcal{N}) = (1-2p)^+ \log d_A$ is the single-letter quantum capacity for this channel [45] (see also Ref. [6]).

Note that $d_A^k \times \rho^{AA'_1 \dots A'_{n-k}}$ is a projector of rank d_A^k . This may be a well-known observation and is not difficult to prove but for the sake of completeness, we provide a proof in the appendix in Lemma 10. Observe that $\rho^{A'_1 \dots A'_{n-k}}$ is the maximally mixed state. We note that the capacity-achieving input is maximally entangled.

For reasons that should be apparent from what follows, we also consider λ -quasi relative entropy for $\lambda \in [0, 2] \setminus \{1\}$ given by

$$D_{\lambda}^{\text{quasi}}(\rho||\sigma) := \text{sign}(\lambda - 1) \text{Tr} \rho^{\lambda} \sigma^{1-\lambda}. \quad (105)$$

This relative entropy is jointly convex in its arguments and satisfies monotonicity for the chosen range of λ [28]. The Rényi divergence is a function of this quantity.

For the hockey-stick divergence and λ -quasi relative entropy, note the following identical steps

$$\mathcal{D}(\rho^{AB^n} || \mathbb{1} \otimes \rho^{B^n}) \stackrel{a}{=} \sum_{2^n \text{ terms}} \alpha_{k,n} \mathcal{D}(\zeta_{i_1, \dots, i_{n-k}}^{AB_{i_1} \dots B_{i_n}} || \mathbb{1} \otimes \zeta_{i_1, \dots, i_{n-k}}^{B_{i_1} \dots B_{i_n}}) \quad (106)$$

$$\stackrel{b}{=} \sum_{2^n \text{ terms}} \alpha_{k,n} \mathcal{D}(\sigma^{AB_{i_1} \dots B_{i_{n-k}}} || \mathbb{1} \otimes \sigma^{B_{i_1} \dots B_{i_{n-k}}}) \quad (107)$$

$$\stackrel{c}{\leq} \sum_{2^n \text{ terms}} \alpha_{k,n} \mathcal{D}(\rho^{AA'_{i_1} \dots A'_{i_{n-k}}} || \mathbb{1} \otimes \rho^{A'_{i_1} \dots A'_{i_{n-k}}}), \quad (108)$$

where a follows from orthogonality of ζ 's, b follows since we have removed the tensors with $|e\rangle\langle e|$, and c follows from monotonicity.

The quantity $\mathcal{K}^{(q)}(A; B^n)$ can be upper bounded by $\mathcal{D}(\rho^{AB^n} || \mathbb{1} \otimes \rho^{B^n})$. For the Rényi divergence of order $\lambda \in (1, 2]$, $\mathcal{K}^{(q)}(A; B^n)$ is upper bounded by first computing (108) for the λ -quasi relative entropy to get

$$\mathcal{K}^{(q)}(A; B^n) \leq \frac{n}{\lambda - 1} \log \left[p d_A^{1-\lambda} + (1-p) d_A^{\lambda-1} \right]. \quad (109)$$

Using (81), we get

$$\mathbb{F} \leq \exp \left(-\frac{\lambda - 1}{\lambda} n \left\{ \mathcal{R} - \frac{\log \left[p d_A^{1-\lambda} + (1-p) d_A^{\lambda-1} \right]}{\lambda - 1} \right\} \right). \quad (110)$$

The function

$$h(x) := \log \left[p d_A^{1-x} + (1-p) d_A^{x-1} \right] \quad (111)$$

satisfies $h(1) = 0$. Furthermore, for $p \in [0, 1/2]$,

$$\lim_{\lambda \downarrow 1} \frac{h(\lambda)}{\lambda - 1} = Q(\mathcal{N}). \quad (112)$$

Hence, for all $\mathcal{R} > Q(\mathcal{N})$, $\exists \lambda \in (1, 2]$ s.t. $\mathcal{R} - h(\lambda)/(\lambda - 1) > 0$, and thus the strong converse holds. For $p > 1/2$, $h'(1) < 0$ and hence, using similar arguments as above, the strong converse follows.

For the hockey-stick divergence, (108) is computed as

$$\mathcal{K}^{(q)}(A; B^n) \leq \sum_{k=0}^n \binom{n}{k} \alpha_{k,n} \text{Tr} \left(\rho^{AA'_{i_1} \dots A'_{i_{n-k}}} - \gamma \mathbb{1} \otimes \rho^{A'_{i_1} \dots A'_{i_{n-k}}} \right)^+ \quad (113)$$

$$\leq \sum_{k=0}^{\frac{n}{2} - \lfloor \frac{\log \gamma}{2 \log d_A} \rfloor} \binom{n}{k} \alpha_{k,n}, \quad (114)$$

where we have upper bounded $\text{Tr}(\rho^{AA'_1 \dots A'_{n-k}} - \gamma \mathbb{1} \otimes \rho^{A'_1 \dots A'_{n-k}})^+$ by 1 for $k \leq n/2 - \lfloor \log \gamma / (2 \log d_A) \rfloor$.

Let us choose $\log \gamma = n[\mathcal{R} + Q(\mathcal{N})]/2$ in (108). For $\mathcal{R} > Q(\mathcal{N})$, we have $n/2 - \lfloor \log \gamma / (2 \log d_A) \rfloor < np$. Using the Chernoff bound and (93), we get

$$\mathbb{F} \leq \exp \left\{ -\frac{n}{2} [\mathcal{R} - Q(\mathcal{N})] \right\} + \exp \left\{ -\frac{n}{2p} \left[\frac{(2p-1)^+}{2} + \frac{\mathcal{R}}{4 \log d_A} \right]^2 \right\}, \quad (115)$$

which gives us the strong converse.

V. ACKNOWLEDGEMENT

The authors gratefully acknowledge the comments by A. Winter.

-
- [1] C. E. Shannon, "A mathematical theory of communication," *Bell Sys. Tech. J.*, vol. 27, pp. 379–423 and 623–656, July and Oct. 1948.
 - [2] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 2nd ed., 2006.
 - [3] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. New York, USA: Cambridge University Press, 2nd ed., 2011.
 - [4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.
 - [5] M. Hayashi, *Quantum Information: An Introduction*. Berlin: Springer, 2006.
 - [6] M. M. Wilde, "From classical to quantum Shannon theory." <http://arxiv.org/abs/1106.1445>, 2011.
 - [7] R. G. Gallager, *Information Theory and Reliable Communication*. New York: John Wiley & Sons, Inc., 1968.
 - [8] T. Dorlas and C. Morgan, "The invalidity of a strong capacity for a quantum channel with memory," *Phys. Rev. A*, vol. 84, p. 042318, Oct. 2011.
 - [9] J. Wolfowitz, *Coding Theorems of Information Theory*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1962.
 - [10] S. Arimoto, "On the converse to the coding theorem for discrete memoryless channels," *IEEE Trans. Inf. Theory*, vol. 19, pp. 357 – 359, May 1973.
 - [11] R. G. Gallager, "A simple derivation of the coding theorem and some applications," *IEEE Trans. Inf. Theory*, vol. 11, pp. 3–18, Jan. 1965.
 - [12] A. S. Holevo, "The capacity of a quantum channel with general signal states," *IEEE Trans. Inf. Theory*, vol. 22, pp. 269–273, Jan. 1998.
 - [13] B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy classical channels," *Phys. Rev. A*, vol. 56, pp. 131–138, July 1997.
 - [14] M. B. Hastings, "Superadditivity of communication capacity using entangled inputs," *Nat. Phys.*, vol. 5, pp. 255–257, Mar. 2009.
 - [15] A. Winter, "Coding theorem and strong converse for quantum channels," *IEEE Trans. Inf. Theory*, vol. 45, pp. 2481–2485, Nov. 1999.
 - [16] T. Ogawa and H. Nagaoka, "Strong converse to the quantum channel coding theorem," *IEEE Trans. Inf. Theory*, vol. 45, pp. 2486–2489, Nov. 1999.
 - [17] R. König and S. Wehner, "A strong converse for classical channel coding using entangled inputs," *Phys. Rev. Lett.*, vol. 103, p. 070504, Aug. 2009.
 - [18] T. S. Han and K. Kobayashi, "The strong converse theorem for hypothesis testing," *IEEE Trans. Inf. Theory*, vol. 35, pp. 178–180, Jan. 1989.
 - [19] T. Ogawa and H. Nagaoka, "Strong converse theorems in the quantum information theory," in *Proc. Inf. Theory Net. Work. (ITNW)*, (Metsovo, Greece), June 1999.

- [20] T. Ogawa and H. Nagaoka, “Strong converse and Stein’s lemma in quantum hypothesis testing,” *IEEE Trans. Inf. Theory*, vol. 46, pp. 2428–2433, Nov. 2000.
- [21] R. Ahlswede and A. Winter, “Strong converse for identification via quantum channels,” *IEEE Trans. Inf. Theory*, vol. 48, pp. 569–579, Mar. 2002.
- [22] R. Ahlswede and N. Cai, “A strong converse theorem for quantum multiple access channels,” *Electronic Notes in Discrete Mathematics*, vol. 21, pp. 137 – 141, 2005.
- [23] Y. Polyanskiy, H. V. Poor, and S. Verdú, “Channel coding rate in the finite block length regime,” *IEEE Trans. Inf. Theory*, vol. 56, pp. 2307–2359, May 2010.
- [24] Y. Polyanskiy and S. Verdú, “Arimoto channel coding converse and Rényi divergence,” in *Proc. 48th Allerton Conf. Comm. Cont. Comp.*, (Monticello, USA), Sept. 2010.
- [25] R. E. Blahut, “Information bounds of the Fano-Kullback type,” *IEEE Trans. Inf. Theory*, vol. 22, pp. 410–421, July 1976.
- [26] T. S. Han and S. Verdú, “Generalizing the Fano inequality,” *IEEE Trans. Inf. Theory*, vol. 40, pp. 1247–1251, July 1994.
- [27] I. Csiszár, “Generalized cutoff rates and Rényi’s information measures,” *IEEE Trans. Inf. Theory*, vol. 41, pp. 26–34, Jan. 1995.
- [28] M. Mosonyi and F. Hiai, “On the quantum Rényi relative entropies and related capacity formulas,” *IEEE Trans. Inf. Theory*, vol. 57, pp. 2474–2487, April 2011.
- [29] N. Sharma, “Extensions of the quantum Fano inequality,” *Phys. Rev. A*, vol. 78, p. 012322, July 2008.
- [30] F. Hiai, M. Mosonyi, D. Petz, and C. Bény, “Quantum f -divergences and error correction,” *Rev. Math. Phys.*, vol. 23, pp. 691–747, 2011.
- [31] J. Hull, *Options, Futures, and Other Derivatives*. Upper SaddleRiver, NJ, USA: Prentice Hall, 5th ed., 2003.
- [32] A. Lesniewski and M. B. Ruskai, “Monotone Riemannian metrics and relative entropy on noncommutative probability spaces,” *J. Math. Phys.*, vol. 40, pp. 5702–24, Nov. 1999.
- [33] N. Sharma, “Equality conditions for the quantum f -relative entropy and generalized data processing inequalities,” *Quant. Inf. Process.*, vol. 11, pp. 137–160, Feb. 2012.
- [34] A function $f(x)$ is said to be operator convex if for any two Hermitian matrices ρ and σ with spectrum in the domain of f and any $\lambda \in [0, 1]$, we have $f[\lambda\rho + (1 - \lambda)\sigma] \leq \lambda f(\rho) + (1 - \lambda)f(\sigma)$, where we say $\rho \leq \sigma$, if $\sigma - \rho$ is positive semi-definite [46].
- [35] Note that whether or not $C^{(1)}(\mathcal{N})$ is the channel capacity is intimately tied to the question of additivity (see Ref. [14] and references therein).
- [36] B. Schumacher, “Sending entanglement through noisy quantum channels,” *Phys. Rev. A*, vol. 54, pp. 2614–2628, Oct. 1996.
- [37] B. Schumacher and M. A. Nielsen, “Quantum data processing and error correction,” *Phys. Rev. A*, vol. 54, pp. 2629–2635, Oct. 1996.
- [38] H. Barnum, M. A. Nielsen, and B. Schumacher, “Information transmission through a noisy quantum channel,” *Phys. Rev. A*, vol. 57, pp. 4153–4175, June 1998.
- [39] H. Barnum, E. Knill, and M. A. Nielsen, “On quantum fidelities and channel capacities,” *IEEE Trans. Inf. Theory*, vol. 46, pp. 1317–1329, July 2000.
- [40] S. Lloyd, “Capacity of the noisy quantum channel,” *Phys. Rev. A*, vol. 55, pp. 1613–1622, Mar. 1997.
- [41] P. W. Shor, “The quantum channel capacity and coherent information,” in *MSRI Workshop on Quantum Computation*, (<http://www.msri.org/publications/ln/msri/2002/quantumcrypto/shor/1/>), 2002.
- [42] I. Devetak, “The private classical capacity and quantum capacity of a quantum channel,” *IEEE Trans. Inf. Theory*, vol. 51, pp. 44–55, Jan. 2005.
- [43] P. Hayden, P. W. Shor, and A. Winter, “Random quantum codes from Gaussian ensembles and an uncertainty relation,” *Open Syst. Inf. Dyn.*, vol. 15, pp. 71–89, Mar. 2008.
- [44] M. Grassl, Th. Beth, and T. Pellizzari, “Codes for the quantum erasure channel,” *Phys. Rev. A*, vol. 56, pp. 33–38, July 1997.
- [45] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin, “Capacities of quantum erasure channels,” *Phys. Rev. Lett.*, vol. 78, pp. 3217–3230, Apr. 1997.

- [46] R. Bhatia, *Matrix Analysis*. New York: Springer-Verlag, 1997.
- [47] M. Ohya and D. Petz, *Quantum Entropy and its use*. Berlin: Springer-Verlag, 1st ed., 1993.
- [48] K. M. R. Audenaert, J. Calsamiglia, Ll. Masanes, R. Muñoz-Tapia, A. Acín, E. Bagan, and F. Verstraete, “Discriminating states: The quantum Chernoff bound,” *Phys. Rev. Lett.*, vol. 98, p. 160501, Apr. 2007.
- [49] R. Sibson, “Information radius,” *Prob. Theory Rel. Fields*, vol. 14, pp. 149–160, 1969.
- [50] J. M. Leinaas, J. Myrheim, and E. Ovrum, “Extreme points of the set of density matrices with positive partial transpose,” *Phys. Rev. A*, vol. 76, p. 034304, Sep 2007.

Appendix A: Proof of Lemmas

Lemma 4. *Consider the matrices $\rho, \sigma \geq 0$ and a scalar $\gamma > 0$. Then for any CPTP map \mathcal{E} ,*

$$\text{Tr}(\rho - \gamma\sigma)^+ \geq \text{Tr}[\mathcal{E}(\rho) - \gamma\mathcal{E}(\sigma)]^+. \quad (\text{A1})$$

Proof. Let the Jordan decomposition of $\rho - \gamma\sigma = Q - S$, where $Q, S \geq 0$. Let $P := P_{\{\mathcal{E}(\rho) - \gamma\mathcal{E}(\sigma) \geq 0\}}$. Then

$$\text{Tr}(\rho - \gamma\sigma)^+ = \text{Tr}Q \quad (\text{A2})$$

$$\stackrel{a}{=} \text{Tr}\mathcal{E}(Q) \quad (\text{A3})$$

$$\stackrel{b}{\geq} \text{Tr}P[\mathcal{E}(Q) - \mathcal{E}(S)] \quad (\text{A4})$$

$$= \text{Tr}[\mathcal{E}(\rho) - \gamma\mathcal{E}(\sigma)]^+, \quad (\text{A5})$$

where a follows since \mathcal{E} is trace preserving, b follows since we are subtracting non-negative terms. \square

Lemma 5. *Let $f : \mathbb{R}^+ \rightarrow \mathbb{R}$ be an operator monotone function. Then for $\rho, \sigma \geq 0$, $P := P_{\{\rho - \sigma \geq 0\}}$, we have*

$$\text{Tr}P\rho[f(\rho) - f(\sigma)] \geq 0. \quad (\text{A6})$$

Proof. We follow the arguments similar to Theorem 11.18 in Ref. [47] (see also the proof of Lemma 1 in Ref. [48]). Using the Löwner’s Theorem (see Ref. [47]),

$$f(x) = \int_0^\infty \frac{x(1+\lambda)}{x+\lambda} d\mu(\lambda), \quad (\text{A7})$$

where μ is a positive finite measure, we get

$$\text{Tr}P\rho[f(\rho) - f(\sigma)] = \int_0^\infty \lambda(1+\lambda) \text{Tr}[P\rho(\rho+\lambda)^{-1}(\rho-\sigma)(\sigma+\lambda)^{-1}] d\mu(\lambda). \quad (\text{A8})$$

To prove the inequality, it is sufficient to show that $\text{Tr}P\rho(\rho+\lambda)^{-1}(\rho-\sigma)(\sigma+\lambda)^{-1} \geq 0 \forall \lambda > 0$. For $\Delta = \rho - \sigma$, we can get the integral representation

$$\text{Tr}P\rho(\rho+\lambda)^{-1}(\rho-\sigma)(\sigma+\lambda)^{-1} = \int_0^1 \lambda \text{Tr}[P\rho(\sigma+t\Delta+\lambda)^{-1}\Delta(\sigma+t\Delta+\lambda)^{-1}] dt. \quad (\text{A9})$$

Hence, it is sufficient to show that

$$\text{Tr}P\rho(\sigma+t\Delta+\lambda)^{-1}\Delta(\sigma+t\Delta+\lambda)^{-1} \geq 0. \quad (\text{A10})$$

It is shown in Theorem 11.18 in Ref. [47] that $\text{Tr} P \sigma (\sigma + t\Delta + \lambda)^{-1} \Delta (\sigma + t\Delta + \lambda)^{-1} \geq 0$. Now it is easy to see that $\text{Tr} P \Delta (\sigma + t\Delta + \lambda)^{-1} \Delta (\sigma + t\Delta + \lambda)^{-1} = \text{Tr} P [\Delta (\sigma + t\Delta + \lambda)^{-1}]^2 \geq 0$. Adding these two quantities, we get (A10) and the result follows. In particular, since \log is an operator monotone function, the claim implies that

$$\text{Tr} P \rho (\log \rho - \log \sigma) \geq 0. \quad (\text{A11})$$

□

Lemma 6. *Let $\rho, \sigma \geq 0$, $P = P_{\{\rho - \gamma\sigma \geq 0\}}$, and $\log \gamma > S(\rho||\sigma)$, then*

$$\text{Tr} P \rho \leq \frac{\text{Tr} \rho (\log \rho - \log \sigma)^2 - [S(\rho||\sigma)]^2}{[\log \gamma - S(\rho||\sigma)]^2}. \quad (\text{A12})$$

Proof. We can rewrite (A12) as

$$\text{Tr} P \rho \leq \frac{\text{Tr} \rho \{\log \rho - \log(\gamma\sigma) + [\log \gamma - S(\rho||\sigma)] \mathbb{1}\}^2}{[\log \gamma - S(\rho||\sigma)]^2}. \quad (\text{A13})$$

It suffices to show that

$$\text{Tr} P \rho \stackrel{a}{\leq} \frac{\text{Tr} P \rho \{\log \rho - \log(\gamma\sigma) + [\log \gamma - S(\rho||\sigma)] \mathbb{1}\}^2}{[\log \gamma - S(\rho||\sigma)]^2} \quad (\text{A14})$$

$$= \frac{\text{Tr} P \rho [\log \rho - \log(\gamma\sigma)]^2}{[\log \gamma - S(\rho||\sigma)]^2} + \frac{\text{Tr} P \rho [\log \rho - \log(\gamma\sigma)]}{[\log \gamma - S(\rho||\sigma)]} + \text{Tr} P \rho, \quad (\text{A15})$$

where in *a*, the sufficient condition is due to multiplication by P . The first term is non-negative and the second term is non-negative using Lemma 5 and the inequality follows. □

Lemma 7 (Quantum Sibson identity). *For any quantum state ρ^{AB} in system AB and D_λ to be the Rényi divergence of order λ , we have*

$$D_\lambda(\rho^{AB}||\mathbb{1} \otimes \sigma^B) = D_\lambda(\sigma^*||\sigma^B) + \frac{\lambda}{\lambda-1} \log \text{Tr} \left[\text{Tr}_A (\rho^{AB})^\lambda \right]^{\frac{1}{\lambda}}, \quad (\text{A16})$$

$$\text{where } \sigma^* = \frac{\left[\text{Tr}_A (\rho^{AB})^\lambda \right]^{\frac{1}{\lambda}}}{\text{Tr} \left[\text{Tr}_A (\rho^{AB})^\lambda \right]^{\frac{1}{\lambda}}}. \quad (\text{A17})$$

Proof. For the classical Sibson identity, see Ref. [49]. Note that

$$D_\lambda(\rho^{AB}||\mathbb{1} \otimes \sigma^B) = \frac{1}{\lambda-1} \log \text{Tr} (\rho^{AB})^\lambda [\mathbb{1} \otimes (\sigma^B)^{1-\lambda}] \quad (\text{A18})$$

$$= \frac{1}{\lambda-1} \log \text{Tr} \text{Tr}_A (\rho^{AB})^\lambda (\sigma^B)^{1-\lambda} \quad (\text{A19})$$

$$= \frac{1}{\lambda-1} \log \text{Tr} (\sigma^*)^\lambda (\sigma^B)^{1-\lambda} + \frac{\lambda}{\lambda-1} \log \text{Tr} \left[\text{Tr}_A (\rho^{AB})^\lambda \right]^{\frac{1}{\lambda}} \quad (\text{A20})$$

$$= D_\lambda(\sigma^*||\sigma^B) + \frac{\lambda}{\lambda-1} \log \text{Tr} \left[\text{Tr}_A (\rho^{AB})^\lambda \right]^{\frac{1}{\lambda}}. \quad (\text{A21})$$

□

Lemma 8. If $\mathcal{R} > \max_{\rho^{AA'}} I(A)B)_\sigma$, then

$$\exists t \in [-1/2, 0), \text{ such that } \forall s \in (t, 0), \quad -s\mathcal{R} + \min_{\rho^{AA'}} E_0(s, \mathcal{N})_\rho > 0. \quad (\text{A22})$$

Proof. The proof follows the same argument as Lemma 3 in Ref. [16]. Let $g(s, \rho^{AA'}) := -s\mathcal{R} + E_0(s, \mathcal{N})_\rho$ and suppose that $\mathcal{R} > \max_{\rho^{AA'}} I(A)B)_\sigma$. Note that $\forall \rho^{AA'}$ we have $g(0, \rho^{AA'}) = 0$ and

$$g'(0, \rho^{AA'}) = -\mathcal{R} + I(A)B)_\sigma < 0. \quad (\text{A23})$$

Now suppose that (A22) does not hold. Then

$$\forall t \in [-1/2, 0), \quad \exists s \in (t, 0), \quad \text{such that } \min_{\rho^{AA'}} g(s, \rho^{AA'}) \leq 0. \quad (\text{A24})$$

Hence, there exists a real sequence $\{s_n\}$ and a sequence $\{\rho_n^{AA'}\} \subset \mathcal{S}(\mathcal{H}_{AA'})$ such that

$$s_n \in \left(-\frac{1}{n+1}, 0\right) \quad \text{and} \quad g(s_n, \rho_n^{AA'}) \leq 0. \quad (\text{A25})$$

Now since $\mathcal{S}(\mathcal{H}_{AA'})$ is a compact set (see Ref. [50]), there exists a subsequence of $\{\rho_n^{AA'}\}$ that converges to some $\rho_\infty^{AA'}$ as $n \rightarrow \infty$. Without loss of generality we can assume that $\rho_n^{AA'} \rightarrow \rho_\infty^{AA'}$. From the mean value theorem, it follows that

$$\forall n, \quad \exists r_n \in (s_n, 0), \quad \text{such that } g'(r_n, \rho_n^{AA'}) = \frac{g(0, \rho_n^{AA'}) - g(s_n, \rho_n^{AA'})}{0 - s_n} \geq 0. \quad (\text{A26})$$

Since $g'(s, \rho^{AA'})$ is a continuous function of $(s, \rho^{AA'})$, (A26) yields $g'(0, \rho_\infty^{AA'}) \geq 0$, which contradicts (A23). \square

Lemma 9. Consider a cq-state $\rho^{AB} = \sum_x P_X(x) |x\rangle\langle x|^A \otimes \sigma_x^B$, where P_X is a probability distribution and $\sigma_x^B \in \mathcal{S}(\mathcal{H}_B)$. Then for all such cq-states,

$$\text{Tr} \rho^{AB} [\log \rho^{AB} - \log(\rho^A \otimes \rho^B)]^2 \leq g(|AB|) + g(|B|), \quad (\text{A27})$$

where for any $d \in \mathbb{N}$, $g(1) = 0$,

$$g(d) := \begin{cases} 0.563, & d = 2 \\ \log^2 d, & d \geq 3. \end{cases} \quad (\text{A28})$$

Proof. It is not difficult to see that for $\rho^A = \text{Tr}_B \rho^{AB}$, $\rho^B = \text{Tr}_A \rho^{AB}$,

$$[\log \rho^{AB} - \log(\rho^A \otimes \rho^B)]^2 = \log^2 \rho^{AB} - \log^2 \rho^A \otimes \mathbb{1} + \mathbb{1} \otimes \log^2 \rho^B \quad (\text{A29})$$

$$- 2 \sum_x \log P_X(x) |x\rangle\langle x|^A \otimes \log \sigma_x^B \quad (\text{A30})$$

$$- \sum_x |x\rangle\langle x|^A \otimes (\log \sigma_x^B \log \rho^B + \log \rho^B \log \sigma_x^B). \quad (\text{A31})$$

Each term above with the negative sign contributes negatively when we take the trace and hence, neglecting these terms gives us an upper bound. We are left with

$$\text{Tr} \rho^{AB} \log^2 \rho^{AB} + \text{Tr} \rho^B \log^2 \rho^B. \quad (\text{A32})$$

Using the arguments in Appendix E in Ref. [23], it follows that for a quantum state σ of dimension d , $\text{Tr} \sigma \log^2 \sigma \leq g(d)$. QED. \square

Lemma 10. *Let $|\psi\rangle^{XY_1Y_2}$ be a maximally entangled state, i.e.,*

$$|\psi\rangle^{XY_1Y_2} = \frac{1}{\sqrt{|Y_1||Y_2|}} \sum_{i_1=1}^{|Y_1|} \sum_{i_2=1}^{|Y_2|} |i_1 i_2\rangle^X |i_1 i_2\rangle^{Y_1 Y_2}, \quad (\text{A33})$$

where $|X| \geq |Y_1||Y_2|$, $\{|i_1 i_2\rangle^X\}$ and $\{|i_1 i_2\rangle^{Y_1 Y_2}\}$ are any orthonormal bases in \mathcal{H}_X and $\mathcal{H}_{Y_1} \otimes \mathcal{H}_{Y_2}$ respectively. Then, $|Y_2| \rho^{XY_1}$ is a projector where $\rho^{XY_1} = \text{Tr}_{Y_2} \psi^{XY_1 Y_2}$.

Proof. It is easy to see that

$$\rho^{XY_1} = \frac{1}{|Y_1||Y_2|} \sum_{i_1, i'_1=1}^{|Y_1|} \sum_{i_2, i'_2=1}^{|Y_2|} |i_1 i_2\rangle \langle i'_1 i'_2|^X \otimes \text{Tr}_{Y_2} (|i_1 i_2\rangle \langle i'_1 i'_2|^{Y_1 Y_2}). \quad (\text{A34})$$

To prove the claim, it suffices to show that $(|Y_2| \rho^{XY_1})^2 = |Y_2| \rho^{XY_1}$ or

$$\frac{1}{|Y_1|} \sum_{j_1=1}^{|Y_1|} \sum_{j_2=1}^{|Y_2|} \text{Tr}_{Y_2} (|i_1 i_2\rangle \langle j_1 j_2|^{Y_1 Y_2}) \text{Tr}_{Y_2} (|j_1 j_2\rangle \langle j'_1 j'_2|^{Y_1 Y_2}) = \text{Tr}_{Y_2} (|i_1 i_2\rangle \langle j'_1 j'_2|^{Y_1 Y_2}). \quad (\text{A35})$$

Now consider the Schmidt decomposition of $|i_1 i_2\rangle^{Y_1 Y_2}$, i.e.,

$$|i_1 i_2\rangle^{Y_1 Y_2} = \sum_k \sqrt{\alpha_{k i_1 i_2}} |k i_1 i_2\rangle^{Y_1} |k i_2 i_2\rangle^{Y_2}. \quad (\text{A36})$$

Substituting in (A35) and simplifying, we have

$$\text{LHS of (A35)} = \frac{1}{|Y_1|} \sum_{j_1, j_2, k, l, l'} \sqrt{\alpha_{k i_1 i_2} \alpha_{l' j'_1 j'_2}} \alpha_{l j_1 j_2} \langle l' j'_1 j'_2 | l j_1 j_2 \rangle^{Y_2} \langle l j_1 j_2 | k i_1 i_2 \rangle^{Y_2} |k i_1 i_2\rangle \langle l' j'_1 j'_2|^{Y_1} \quad (\text{A37})$$

$$= \sum_{k, l'} \sqrt{\alpha_{k i_1 i_2} \alpha_{l' j'_1 j'_2}} \langle l' j'_1 j'_2 |^{Y_2} \left(\frac{1}{|Y_1|} \sum_{j_1, j_2, l} \alpha_{l j_1 j_2} |l j_1 j_2\rangle \langle l j_1 j_2|^{Y_2} \right) |k i_1 i_2\rangle^{Y_2} |k i_1 i_2\rangle \langle l' j'_1 j'_2|^{Y_1} \quad (\text{A38})$$

$$\stackrel{a}{=} \sum_{k, l'} \sqrt{\alpha_{k i_1 i_2} \alpha_{l' j'_1 j'_2}} \langle l' j'_1 j'_2 |^{Y_2} |k i_1 i_2\rangle^{Y_2} |k i_1 i_2\rangle \langle l' j'_1 j'_2|^{Y_1} \quad (\text{A39})$$

$$= \text{RHS of (A35)}, \quad (\text{A40})$$

where in a , we have replaced the term inside the parenthesis by an identity matrix since

$$\frac{1}{|Y_1|} \sum_{j_1, j_2, l} \alpha_{l j_1 j_2} |l j_1 j_2\rangle \langle l j_1 j_2|^{Y_2} = \frac{1}{|Y_1|} \sum_{j_1, j_2} \text{Tr}_{Y_1} (|l j_1 j_2\rangle \langle l j_1 j_2|^{Y_1 Y_2}) = \mathbb{1}. \quad (\text{A41})$$

QED. \square

Appendix B: Proof of Theorem 5

Note that (85) follows easily. We now verify (86) using the following differentiation rule (Lemma 4 in Ref. [16]) for a Hermitian operator $X(s)$ parametrized by a real parameter s

$$\frac{\partial}{\partial s} \text{Tr} g[X(s)] = \text{Tr} g'[X(s)] \frac{\partial X(s)}{\partial s}. \quad (\text{B1})$$

Let the spectral decomposition of σ^{AB} be $\sigma^{AB} = \sum_i \lambda_i |i\rangle\langle i|^{AB}$ and let $\sigma_i = \text{Tr}_A |i\rangle\langle i|^{AB}$. Hence, we get $\sigma^B = \text{Tr}_A \sigma^{AB} = \sum_i \lambda_i \sigma_i$ and $\kappa_1 := \text{Tr}_A (\sigma^{AB})^{1/(s+1)} = \sum_i \lambda_i^{1/(s+1)} \sigma_i$. It is easy to see using (B1) that $\partial \kappa_1 / \partial s = -\kappa_2 / (s+1)$, where $\kappa_2 = \sum_i \lambda_i^{\frac{1}{s+1}} \log(\lambda_i^{\frac{1}{s+1}}) \sigma_i$. It now follows that

$$\frac{\partial g(s)}{\partial s} = \frac{\text{Tr} \kappa_1^s (\kappa_2 - \kappa_1 \log \kappa_1)}{\text{Tr} \kappa_1^{s+1}}, \quad (\text{B2})$$

$$\left. \frac{\partial g(s)}{\partial s} \right|_{s=0} = \text{Tr} \left[\sum_i \lambda_i (\log \lambda_i) \sigma_i - \left(\sum_i \lambda_i \sigma_i \right) \log \left(\sum_i \lambda_i \sigma_i \right) \right], \quad (\text{B3})$$

$$= H(B)_\sigma - H(A, B)_\sigma, \quad (\text{B4})$$

$$= I(A)B)_\sigma. \quad (\text{B5})$$

Now we show that $g(s) + (s+1) \log |A|$ is an increasing function in s . Consider the operators $E_i = \sqrt{\sigma_i / |A|}$. Then $\sum_i E_i^\dagger E_i = \sum_i \text{Tr}_A |i\rangle\langle i|^{AB} / |A| = \mathbb{1}$. Since x^γ , $\gamma \in (0, 1]$ is operator concave, we have, using the operator Jensen's inequality and for $1/2 \leq \alpha \leq \beta < 1$, $\gamma = \alpha/\beta$,

$$\left(\frac{1}{|A|} \sum_i \lambda_i^{1/\beta} \sigma_i \right)^\beta \leq \left(\frac{1}{|A|} \sum_i \lambda_i^{1/\alpha} \sigma_i \right)^\alpha, \quad (\text{B6})$$

or $g(\alpha - 1) + \alpha \log |A| \leq g(\beta - 1) + \beta \log |A|$.